

Informe de Análisis de amenazas y vulnerabilidades

Sitio analizado: <https://copernic.co/> (Agente de ventas con IA 24/7)

Grupo

Sala Principal: Adolfo Alvarez, Adriana Figueroa, Leandro Cañellas, Lucas Esteban Osorio, Miguel Vargas

Fecha del análisis: 05-06-2025

Tipo de aplicación: Landing Page para agente IA de ventas 24/7.

1. Aplicación Web seleccionada

Funcionalidades observadas

- Chat con agente IA
- Panel de Ingreso de Wordpress (Login)
- Sección Informativa
- Agendamiento para demo

2. Inspección Técnica

Formularios

- Login de wordpress (/wp-admin/)

Url y parámetros visibles

- assistant.copernic.co/sse/post_message
- br.copernic.co/
- assistant.copernic.co/sse/get_response?api_key=j_ALcdNpnsSwKB5i&user_message=test&session_id=8ny0u3v6h5b&ip_address=8.8.8.8&page_title=COPERNIC+-+Custom+AI+implementation&page_url=https%3A%2F%2Fcopernic.co%2F
- /wp-json/wp/v2/users
- /wp-login.php
- /wp-login.php?action=lostpassword
- br.copernic.co/.git/
- br.copernic.co/.env
- br.copernic.co/.ssh/
- br.copernic.co/.gitignore
- m.stripe.com/6

Versionamiento

- PHP 7.4, con soporte hasta el 1 de enero de 2023
- Wordpress versión 6.8.1
- Laravel 5

Comportamiento ante errores

- 404 sin mayor información (no configurado)

Cookies Almacenadas

- (cadendly.com) APISID=LmgrvWEUIPUuUNwE/AA3qIL93i-wYeQKyM
-> Sin HttpOnly



Códigos HTTP Observados

- 200 OK, 201 Created, 304 Not Modified

3. Amenazas potenciales

- Ataque de fuerza bruta en formulario de acceso a plataforma Wordpress.
- Exposición de estructuras de carpetas internas.
- Ejecución de Exploits en vulnerabilidades conocidas en versión de lenguaje de programación PHP y Framework Laravel.
- Abuso de Chat IA al encontrarse la API expuesta.
- Cookie Stealer por falta de parámetros de seguridad.
- Directory Dumping, al encontrarse .git expuesto.
- Potenciales accesos indebidos por SSH al encontrarse expuestos archivos PEM.

4. Vulnerabilidades visibles

Severidad	Descripción
 Crítica	<code>.env</code> y <code>.git/</code> accesibles en producción. Posibilidad de obtener contraseñas, configuraciones y claves privadas.
 Crítica	<code>.ssh/</code> potencialmente contiene claves privadas reutilizadas en entornos de producción.
 Alta	Enumeración de usuarios WordPress activa. Facilita ataques de fuerza bruta dirigidos.
 Media	API expone parámetros sensibles en URL (<code>api_key</code> , <code>ip_address</code> , <code>session_id</code>), lo que puede ser capturado en registros del navegador o intermediarios.
 Media	Directory listing en subdominios secundarios puede revelar archivos internos, logs o configuraciones.
 Baja	Ausencia de headers de seguridad comunes como <code>Content-Security-Policy</code> , <code>X-Frame-Options</code> , etc. (requiere verificación vía escaneo de cabeceras).

5. Buenas prácticas de seguridad propuestas

- En caso de directory listing, una medida correctiva sería no guardar archivos sensibles en carpetas públicas
- Deshabilitar desde el servidor web
- De ser posible mantener actualizada a una versión soportada.
- Mejorar prácticas para proteger rutas, autenticación adicional

6. Reflexión final

El sitio <https://copernic.co/> tiene una propuesta innovadora y atractiva en torno al uso de inteligencia artificial para ventas automatizadas. Sin embargo, actualmente presenta varios puntos críticos en cuanto a seguridad, especialmente por la exposición pública de archivos sensibles y configuraciones internas del sistema. Esto podría permitir a terceros con malas intenciones acceder al servidor o incluso tomar control total de la plataforma.

Además, el uso de una versión antigua de PHP, que ya no recibe actualizaciones de seguridad, hace que el riesgo sea aún mayor, ya que existen vulnerabilidades conocidas que podrían ser explotadas fácilmente.

Antes de abrir el sistema a clientes reales o continuar con su difusión comercial, es fundamental corregir estos problemas. Una revisión técnica a fondo —como una auditoría de seguridad profesional o un test de penetración (pentest)— sería un paso responsable para proteger tanto el proyecto como a sus futuros usuarios.

Capturas de referencia en reconocimiento pasivo

[1] Uso de la herramienta *whois*

```
l:~/Escritorio/Estudio202X/CursoHackingWeb2025/Lab1Docker$ whois copernic.co
Domain Name: copernic.co
Registry Domain ID: REDACTED FOR PRIVACY
Registrar WHOIS Server: whois.ovh.com
Registrar URL: www.ovh.com
Updated Date: 2025-01-06T06:59:38Z
Creation Date: 2019-01-28T10:49:12Z
Registry Expiry Date: 2026-01-28T10:49:12Z
Registrar: OVH sas
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
```

imagen 1.
whois copernic.co

[2] Tecnologías que presenta

The screenshot displays the Wappalizer interface with a purple header. The main content area is divided into two columns. The left column lists various technologies categorized by function, while the right column provides a summary of the detected technologies.

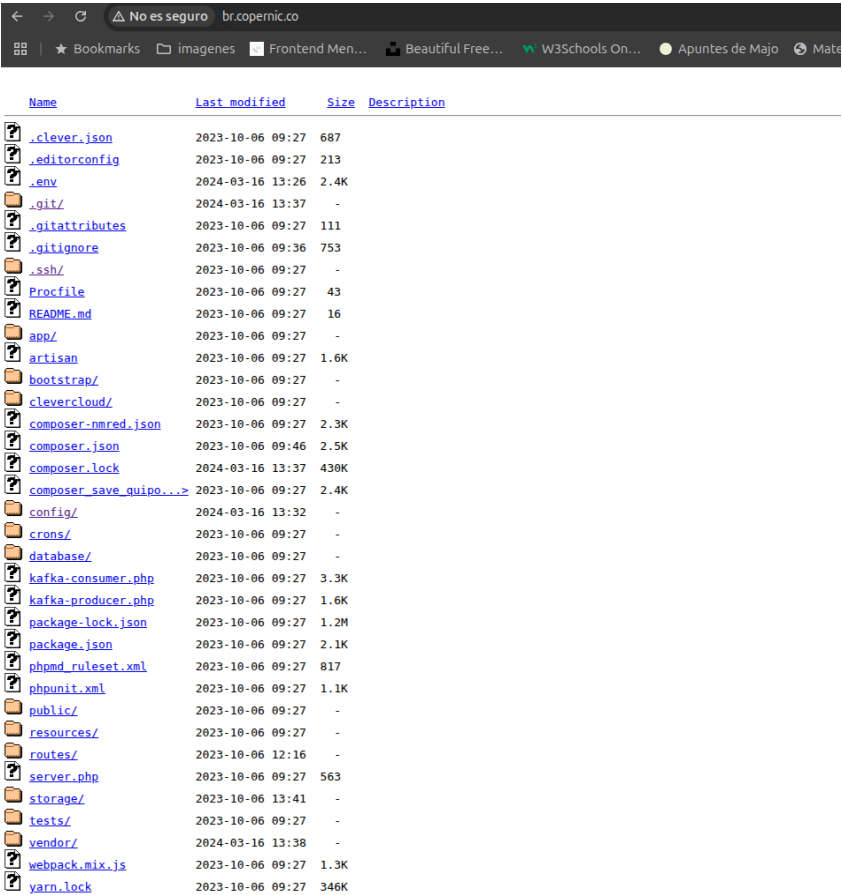
Categoría	Tecnología	Version
Gestor de Contenido	WordPress	6.8.1
	WordPress	6.8.1
Analítica	Plausible	
	LinkedIn Insight Tag	
Blog	WordPress	6.8.1
	WordPress	6.8.1
Tipografía	Google Font API	
	Google Font API	
Librerías JavaScript	Underscore.js	1.13.7
	Clipboard.js	
jQuery UI	jQuery UI	1.13.3
	jQuery UI	1.13.3
core-js	core-js	3.32.0
	core-js	3.32.0
Swiper	Swiper	
	Swiper	
jQuery Migrate	jQuery Migrate	3.4.1
	jQuery Migrate	3.4.1
jQuery	jQuery	3.7.1
	jQuery	3.7.1
Appointment scheduling	Calendly	
	Calendly	

Summary of detected technologies:

- Miscelánea: RSS, Open Graph, LottieFiles 5.6.8
- Lenguaje de programación: PHP 7.4
- Base de Datos: MySQL
- Landing Page Builder: Elementor 3.21.1
- SEO: Yoast SEO
- Temas de WordPress: Hello Elementor 2.8.1
- WordPress plugins: Yoast SEO, Elementor 3.21.1, Polylang
- Traductor: Polylang
- Performance: Priority Hints

imagen 2.
Información recopilada por wappalyzer.

[3] Directory Listing






































Name	Last modified	Size	Description
 .clever.json	2023-10-06 09:27	687	
 .editorconfig	2023-10-06 09:27	213	
 .env	2024-03-16 13:26	2.4K	
 .git/	2024-03-16 13:37	-	
 .gitattributes	2023-10-06 09:27	111	
 .gitignore	2023-10-06 09:36	753	
 .ssh/	2023-10-06 09:27	-	
 Procfile	2023-10-06 09:27	43	
 README.md	2023-10-06 09:27	16	
 app/	2023-10-06 09:27	-	
 artisan	2023-10-06 09:27	1.6K	
 bootstrap/	2023-10-06 09:27	-	
 clevercloud/	2023-10-06 09:27	-	
 composer-nmred.json	2023-10-06 09:27	2.3K	
 composer.json	2023-10-06 09:46	2.5K	
 composer.lock	2024-03-16 13:37	430K	
 composer_save_quipo...>	2023-10-06 09:27	2.4K	
 config/	2024-03-16 13:32	-	
 crons/	2023-10-06 09:27	-	
 database/	2023-10-06 09:27	-	
 kafka-consumer.php	2023-10-06 09:27	3.3K	
 kafka-producer.php	2023-10-06 09:27	1.6K	
 package-lock.json	2023-10-06 09:27	1.2M	
 package.json	2023-10-06 09:27	2.1K	
 phpmd_ruleset.xml	2023-10-06 09:27	817	
 phpunit.xml	2023-10-06 09:27	1.1K	
 public/	2023-10-06 09:27	-	
 resources/	2023-10-06 09:27	-	
 routes/	2023-10-06 12:16	-	
 server.php	2023-10-06 09:27	563	
 storage/	2023-10-06 13:41	-	
 tests/	2023-10-06 09:27	-	
 vendor/	2024-03-16 13:38	-	
 webpack.mix.js	2023-10-06 09:27	1.3K	
 yarn.lock	2023-10-06 09:27	346K	

imagen 3.

[4] Panel de inicio de sesión al wordpress

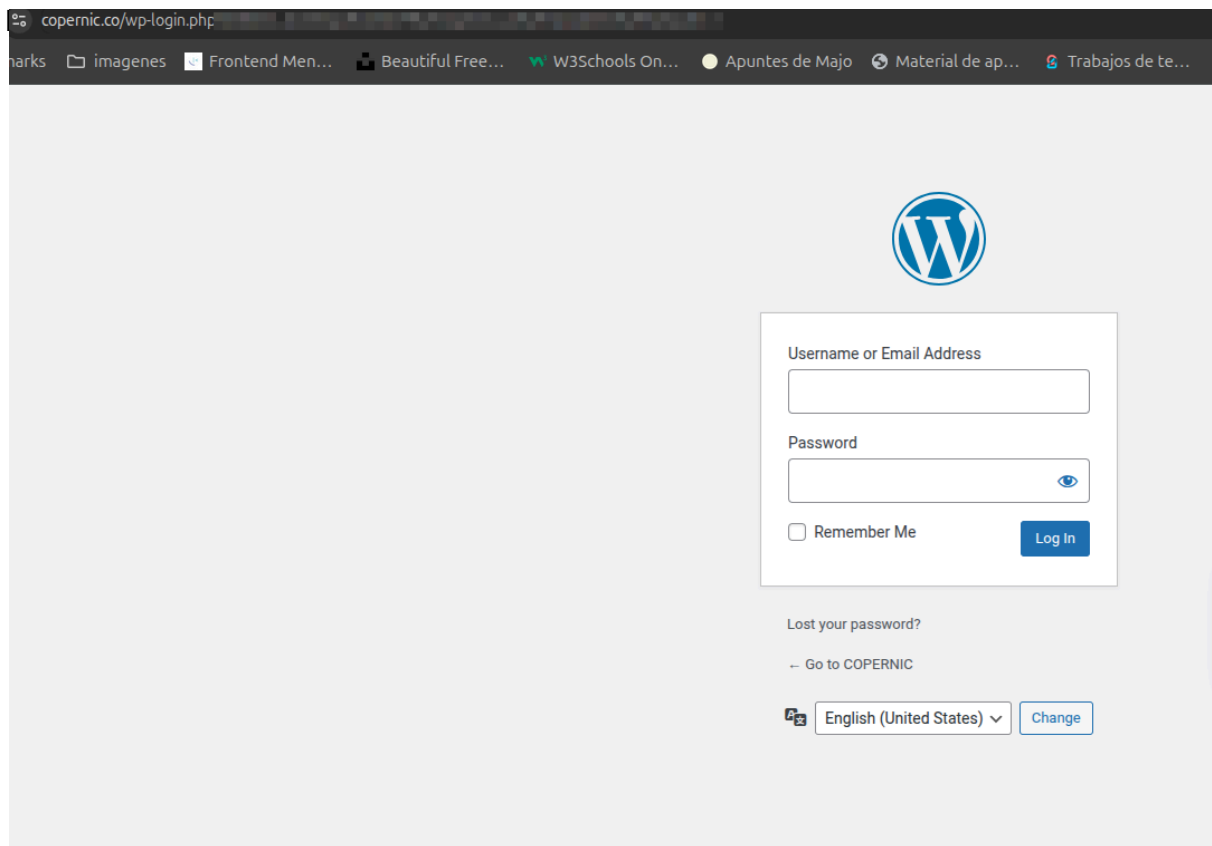


imagen 4.
Panel login, ruta por defecto

[5] Vista pública a un nombre de usuario

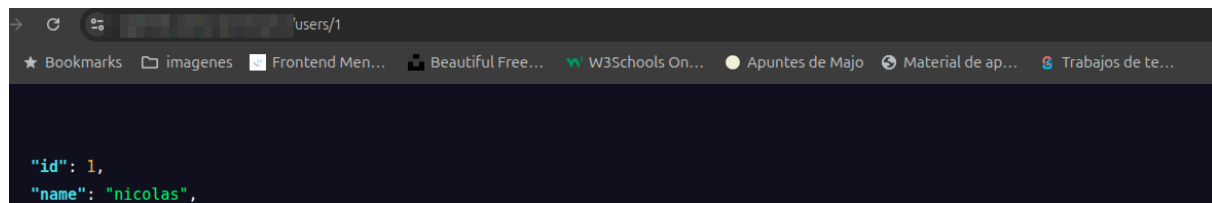


imagen 5.
vista pública a un nombre de usuario.

[6] Key SSH disponible

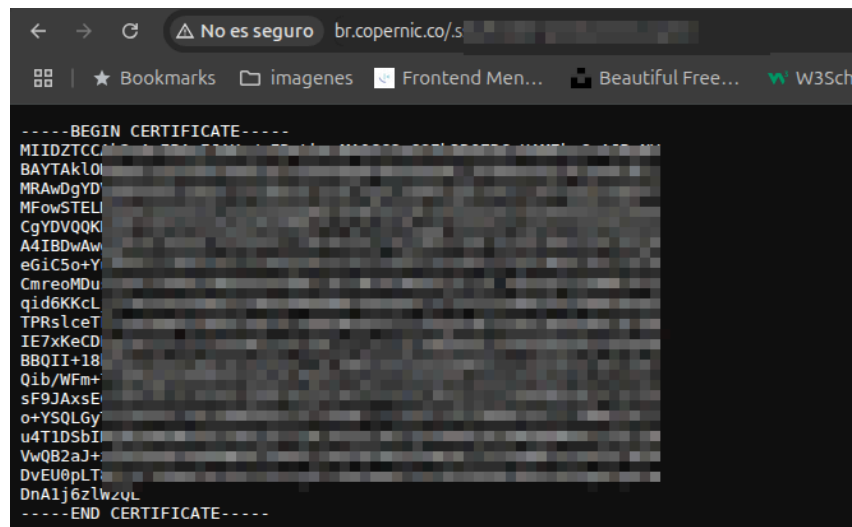


imagen 6.
Key ssh disponibles.